IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

JASON WILLIAMS, Plaintiff, vs. AT&T MOBILITY, LLC, Defendant.	:	Case No.: 5:19-cv-00475-BO

PLAINTIFF JASON WILLIAMS' RESPONSE TO DEFENDANT'S SEPARATE STATEMENT OF UNDISPUTED MATERIAL FACTS, AND PLAINTIFF'S STATEMENT OF ADDITIONAL MATERIAL FACTS

	AT&T's Statement of Undisputed Material Facts and Supporting Evidence	Williams' Responses and Supporting Evidence	Objections
1.	Plaintiff Jason Williams ("Mr. Williams") was an AT&T Mobility wireless telephone subscriber during the relevant period of November 5, 2018 through February 6, 2019. [AT&T's] Appendix 1, Jason Williams Depo., at 271:12-16 (AT&T customer for over 10 years), 73:9-12 (terminated AT&T service in February 2019) and 70:6-10. See also, Complaint (ECF 2) at ¶¶ 1,5, 10-11, 16-17, 35, 120 (Mr. Williams describing his relationship with AT&T as "customer, plan, account, subscriber").	Admitted.	
2.	Mr. Williams' AT&T wireless telephone service was subject to the terms and conditions of the written Wireless Customer Agreement ("WCA"). At true and correct copy of the two WCAs in effect during the relevant period (March 2018 - Nov. 2018, Nov. 2018-Feb. 2019) are attached as Exhibit 3 to the Appendix (no changes to the relevant sections between versions).	Admitted.	Relevance (Fed. R. Evidence 401, 402)

	[AT&T's] Appendix 3, WCAs.		
3.	Mr. Williams executed an acknowledgment that he reviewed and accepted the terms and conditions contained in the Wireless Customer agreement, including its limitations on liability. [AT&T's] Appendix 6, Signed Electronic Acknowledgment, ATT-WIL-01564.	Admitted.	Relevance (Fed. R. Evidence 401, 402)
4.	§4.1 of the WCA states: Unless prohibited by law, AT&T isn't liable for any indirect, special, punitive, incidental or consequential losses or damages you or any third party may suffer by use of, or inability to use, Services, Software, or Devices provided by or through AT&T, including loss of business or goodwill, revenue or profits, or claims of personal injuries. [AT&T's] Appendix 3, Wireless Customer Agreement, § 4.1, What Are The Limitations On Service And Liability?.	Admitted.	Relevance (Fed. R. Evidence 401, 402)
5.	The WCA also states at §4.1: AT&T MAKES NO WARRANTY, EXPRESS OR IMPLIED, OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, SUITABILITY, ACCURACY, SECURITY, OR PERFORMANCE REGARDING ANY SERVICES, SOFTWARE OR GOODS, AND IN NO EVENT SHALL AT&T BE LIABLE, WHETHER OR NOT DUE TO ITS OWN NEGLIGENCE, for any: a. act or omission of a third party; b. mistakes, omissions, interruptions, errors, failures to transmit, delays, or defects in the Services or Software provided by or through us; c. damage or injury caused by the use of Services, Software, or Device, including use in a vehicle;	Admitted.	Relevance (Fed. R. Evidence 401, 402)

	d. claims against you by third parties; e. damage or injury caused by a suspension or termination of Services or Software by AT&T; or f. damage or injury caused by failure or delay in connecting a call to 911 or any other emergency service. Notwithstanding the foregoing, if your Service is interrupted for 24 or more continuous hours by a cause within our control, we will issue you, upon request, a credit equal to a pro-rata adjustment of the monthly Service fee for the time period your Service was unavailable, not to exceed the monthly Service fee. Our liability to you for Service failures is limited solely to the credit set forth above. Unless prohibited by law, AT&T isn't liable for any indirect, special, punitive, incidental or consequential losses or damages you or any third party may suffer by use of, or inability to use, Services, Software, or Devices provided by or through AT&T, including loss of business or goodwill, revenue or profits, or claims of personal injuries. To the full extent allowed by law, you hereby release, indemnify, and hold AT&T and its officers, directors, employees and agents harmless from and against any and all claims of any person or entity for damages of any nature arising in any way from or relating to, directly or indirectly, service provided by AT&T or any person's use thereof (including, but not limited to, vehicular damage and personal injury), INCLUDING CLAIMS ARISING IN WHOLE OR IN PART ROM THE ALLEGED NEGLIGENCE OF AT&T, or any violation by you of this Agreement. This obligation shall survive termination of your Service with AT&T. AT&T is not liable to you		

	for changes in operation, equipment, or technology that cause your Device or Software to be rendered obsolete or require modification. SOME STATES, INCLUDING THE STATE OF KANSAS, DON'T ALLOW DISCLAIMERS OF IMPLIED WARRANTIES OR LIMITS ON REMEDIES FOR BREACH. THEREFORE, THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS AGREEMENT GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE. [AT&T's] Appendix 3, WCAs, §4.1.		
6.	The WCA also states at §4.3 that AT&T does not guarantee security: 4.3 Who Is Responsible For Security? AT&T DOES NOT GUARANTEE SECURITY. Data encryption is available with some, but not all, Services sold by AT&T. [AT&T's] Appendix 3, WCAs, §4.3.	Admitted.	Relevance (Fed. R. Evidence 401, 402)
7.	The AT&T WCA also states that AT&T may make changes to a person's device if those changes are requested by someone who presents the subscriber's information to AT&T. [AT&T's] Appendix 3, WCA, §§ 1.10(b).	Admitted.	Relevance (Fed. R. Evidence 401, 402)
8.	Between November 5, 2018 and February 6, 2019, six SIM swaps were performed on Plaintiff's AT&T wireless telephone. In each instance, AT&T restored his wireless telephone service after he complained to AT&T that he had not requested the SIM change. [AT&T's] Appendix 1, Jason Williams Depo., at 178:13-180:12;	Admitted.	Relevance (Fed. R. Evidence 401, 402)

	184:14-23; Appendix 4, Valerie Scheder Depo., at 115:11-125:5.		
9.	A SIM swap does not entail the transfer of the subscriber's SIM card. A SIM swap simply moves the subscriber's telephone number to a new SIM card, and a fraudulent SIM swap typically involves transfer of the customer's phone number to a SIM card that's inside a wireless device in possession of the fraudster. A SIM swap allows the person gaining control over the wireless device to make and receive voice calls and text messages using the subscriber's assigned wireless number after the swap. A SIM swap alone is not a gateway to CPNI or any other personally identifying information or communications. [AT&T's] Appendix 5, Ray Hill Depo., at 89:15-90:12 (a SIM swap moves the wireless phone number from SIM A to SIM B); [AT&T's] Appendix 4, Valerie Scheder Depo., at 46:21-48:25 REDACTED and 157:25-158:9 ("[CPNI] includes information about what types of services the customer has, rate plans, features on the account, billing data).	Disputed. AT&T produced two separate letters addressed to Mr. Williams, each from a member of AT&T's senior management, in which AT&T admitted that "an employee of one of our service providers accessed your Customer Proprietary Network Information (CPNI) without authorization." (*See* Appendix[1], Exs. 25 and 26. AT&T was and is fully aware that its customers use two-factor authentication, including two-factor authentication involving phone calls and text messages as "an extra security layer" for their online accounts. (*See* Appendix, Ex. 27; Ex. 28.) AT&T was and is fully aware that criminals use unauthorized SIM swaps as a way to bypass their victims' phone and text based two-factor authentication security. (*See* Appendix, Ex. 8; Ex. 9; Ex. 10; Ex. 28; Ex. 7 ¶¶95-96.) Legal conclusions regarding the meaning of CPNI provided by AT&T's fact witnesses are not admissible evidence.	Relevance (Fed. R. Evidence 401, 402); Opinion Testimony by a Lay Witness (Fed. R. Evidence 701
10.	SIM swaps are a regular part of AT&T's provision of wireless telephone services to its customers. See [AT&T's] Appendix 4, Valerie Scheder Depo., at 36:15-38:17 and 72:15-76:14.	Admitted.	Relevance (Fed. R. Evidence 401, 402)

[1] All references to the "Appendix" in Plaintiff's Responses and Supporting Evidence, and Plaintiff's Statement of Additional Material Facts, refer to Plaintiff's Appendix to its Opposition to AT&T's Motion for Summary Judgment.

11.	Customer Proprietary Network Information ("CPNI") includes information about calls made and received such as whether they were local or long distance, time of day of the call, the originating and destination phone numbers, and whether the call was answered or the line was busy. [AT&T's] Appendix 4, Valerie Scheder Depo., at 158:2-9; 47 U.S.C. § 222 (h)(1)(A) (definition of CPNI in Federal Communications Act).	Disputed. AT&T produced two separate letters addressed to Mr. Williams, each from a member of AT&T's senior management, in which AT&T admitted that "an employee of one of our service providers accessed your Customer Proprietary Network Information (CPNI) without authorization." (*See* Appendix, Exs. 25 and 26.) AT&T was and is fully aware that its customers use two-factor authentication, including two-factor authentication involving phone calls and text messages as "an extra security layer" for their online accounts. (*See* Appendix, Ex. 27 at 1-2; Ex. 28.) AT&T was and is fully aware that criminals use unauthorized SIM swaps as a way to bypass their victims' phone and text based two-factor authentication security. (*See* Appendix, Ex. 8; Ex. 9; Ex. 10; Ex. 28; Ex. 7 ¶¶95-96.) Legal conclusions regarding the meaning of CPNI provided by AT&T's fact witnesses are not admissible evidence.	Relevance (Fed. R. Evidence 401, 402); Opinion Testimony by a Lay Witness (Fed. R. Evidence 701)
12.	CPNI is not transferred by AT&T to the person gaining control over the subscriber's wireless telephone number through a SIM swap. In fact, a SIM swap does not involve the transfer of any customer information –it simply entails registering an existing number of a cell phone on a new SIM card. A SIM swap alone is not a gateway to CPNI or any other personally identifying information or communications. [AT&T's] Appendix 5, Ray Hill Depo., at 89:15-90:12 (a SIM swap moves the wireless phone number	Disputed. AT&T produced two separate letters addressed to Mr. Williams, each from a member of AT&T's senior management, in which AT&T admitted that "an employee of one of our service providers accessed your Customer Proprietary Network Information (CPNI) without authorization." (*See* Appendix, Exs. 25 and 26.) AT&T was and is fully aware that its customers use two-factor authentication, including two-	Relevance (Fed. R. Evidence 401, 402); Opinion Testimony by a Lay Witness (Fed. R. Evidence 701)

	from SIM A to SIM B); Appendix 4, Valerie Scheder Depo., at 46:21-48:25 REDACTED and 157:25-158:9 ("[CPNI] includes information about what types of services the customer has, rate plans, features on the account, billing data). 47 U.S.C. §222 (h)(1)(A).	factor authentication involving phone calls and text messages as "an extra security layer" for their online accounts. (*See* Appendix, Ex. 27 at 1-2; Ex. 28.) AT&T was and is fully aware that criminals use unauthorized SIM swaps as a way to bypass their victims' phone and text based two-factor authentication security. (*See* Appendix, Ex. 8; Ex. 9; Ex. 10; Ex. 28; Ex. 7 ¶¶95-96.) Legal conclusions regarding the meaning of CPNI provided by AT&T's fact witnesses are not admissible evidence.	
13.	Apollo Kids Mining, LLC ("AKM") is an active Limited Liability Company registered in Delaware. [AT&T's] Appendix 1, Jason Williams Depo., at 25:19-24, 211:4-13, 231:25-235:25, 237:5-10, 291:20-294:9; [AT&T's] Appendix 7, State of Delaware Department of State website entity registration details, March 25, 2022.	Admitted.	
14.	AKM conducted the crypto-mining activities at issue in this action. It owned the mining rigs. [AT&T's] Appendix 1, Jason Williams Depo., at 25:19-24, 35:5-8 (admitting "SIM swap attacks…most specifically [affected] Apollo Kids Mining") and 231:25-235:25.	Disputed. Mr. Williams was and is the sole member of Apollo Kids Mining, LLC ("Apollo"), through which he operated a successful Bitcoin mining operation. (*See* Appendix, Ex. 3 at 25:19-24; 231:25-235:5; 237:5-19.) Williams was entitled to all of the proceeds from Apollo and its Bitcoin mining operation. (*See* Appendix, Ex. 3.) All of the proceeds from Mr. Williams' Bitcoin mining operation were deposited directly into online cryptocurrency accounts, each of which was accessed via Mr. Williams'	Relevance (Fed. R. Evidence 401, 402)

		personal email, and subject to his sole control. (*See* Appendix, Ex. 13; Ex. 14 at 4-7.)	
15.	AKM is not an AT&T subscriber and Mr. Williams never advised AT&T that AKM was relying on AT&T's security practices for its crypto-mining activities. [AT&T's] Appendix 1, Jason Williams Depo., at 267:14-18 and 268:2-10.	Admitted.	Relevance (Fed. R. Evidence 401, 402)
16.	Mr. Williams does not know who sent him threatening text messages, hacked his social media, email, online storage account, cryptocurrency and financial accounts. Mr. Williams has no evidence that any AT&T employee was involved in these threats or hacks. [AT&T's] Appendix 1, Jason Williams Depo., at 59:18-61:6; 63:8-64:2.	Disputed. Each of the at least six SIM swaps on Mr. Williams' account were intentionally executed by AT&T agents. AT&T employees conducted the SIM swaps to criminals, without which the criminals would not have been able to access Mr. Williams' accounts. Therefore, and as the Court previously held, AT&T employees were directly involved in this threats or hacks. (Appendix, Ex. 1 at ATT-WIL-00678, 668, 658, 649, 647, 641; Ex. 29 at 8.) The November 5, 2018, SIM swap on Mr. Williams' account was performed by an AT&T agent named Stephen Defiore. (*See e.g.* Appendix, Ex. 4 at ATT-WIL-00678; 131:12-134:19.) Defiore was an employee at Prime Communications, an authorized AT&T retailer. (*See* Appendix, Ex. 11 at 2; Appendix, Ex. 12.) AT&T's 30(b)(6) deponent regarding the topic of Mr. Williams' SIM swaps, Ray Hill, testified that Defiore was a "manager." (*See e.g.* Appendix, Ex. 4 at 131:12-134:19.)	Relevance (Fed. R. Evidence 401, 402)

		Documents provided by Prime Communications indicate that Defiore was involved in more than one unauthorized SIM swap, and that he "took full responsibility" for the SIM swaps. (*See e.g.* Appendix, Ex. 12.) This evidence supports the reasonable inference that Defiore, a "manager," intentionally changed Mr. Williams' SIM card on November 5, 2018, without Mr. Williams' authorization, and thereby provided it to a third-party who could use it for whatever purpose they wanted.	
17.	Mr. Williams was reimbursed by First Citizens Bank for all amounts transferred from his First Citizens account to his Coinbase account. [AT&T's] Appendix 1, Jason Williams Depo., at 238:15-239:4.	Admitted.	Relevance (Fed. R. Evidence 401, 402)
18.	Mr. Williams did not seek or obtain any medical or psychological treatment for emotional distress. Mr. Williams does not have any receipts for out-of-pocket expenses related to any claim for emotional distress. Mr. Williams does not have a diary or other record of his alleged emotional distress. [AT&T's] Appendix 1, Jason Williams Depo. at 254:04-254:11; 255:06-255:12 (no counseling or medical treatment) and 252:5-10 (no diary).	Admitted.	Relevance (Fed. R. Evidence 401, 402)
19.	Mr. Williams' complaints of unauthorized SIM swaps leading to alleged losses from cryptocurrency online accounts REDACTED. [AT&T's] Appendix 4, Valerie Scheder Depo., 29:8-21; 30:14-33:25, 36:15-38:17; 39:2-40:3, 45:3-48:25, 52:4-53:5, 57:17-58:6, 72:15-76:14, 77:23-85:15, 86:9-101:1, 104:6-109:2, 109:21-113:22, 177:6-178:15 and 190:4-191:2	Disputed. By November 2018, AT&T knew, or should have known, that unauthorized SIM swaps were serious threats to its customers. (*See* Appendix, Ex. 8; Ex. 9; Ex. 10.) In fact, one of AT&T's own experts indicated in his report that by November 2018, *even AT&T's*	Relevance (Fed. R. Evidence 401, 402)

	(describing series of actions AT&T undertook in response to reports by AT&T customers complaining that SIM swaps being used to gain control of their wireless telephone numbers to steal from their cryptocurrency and other online accounts).	*customers like Mr. Williams* should have been aware of the threat of SIM swaps. (*See* Appendix, Ex. 7 ¶¶95-96) Surely, then, AT&T, as one of the nation's largest telecom providers, was or should have been aware that its customers, including Mr. Williams, could be targeted for SIM swaps in November 2018.	

	Plaintiff's Statement of Additional Material Facts as to Which Plaintiff Contends There is a Genuine Dispute	**AT&T's Responses and Supporting Evidence**	**Objections**
1.	Mr. Williams was an AT&T cellular phone customer in November 2018. (*E.g.* Appendix, Ex. 1 at ATT-WIL-00624-690.)		
2.	On November 5, 2018, Mr. Williams was the victim of a "SIM swap" attack, in which AT&T swapped his SIM card without his authorization. (Appendix, Ex. 2 ATT-WIL00678 (AT&T Account Note entitled "Replace SIM"), 676 (AT&T Account Note entitled "Special Instructions"); Appendix, Ex. 2.)		
3.	As a result of the SIM swap, Mr. Williams lost access to and use of the phone number associated with his AT&T account, and access to and use of that phone number was provided to a third-party. (Appendix, Ex. 3 at 154:8-155:12; *see also* Ex. 4 at 89:15-91:4; AT&T's Memorandum of Law in Support of Defendant's Motion for Summary Judgment, Doc. No. 119 ("AT&T Mov. Br.") at 21.)		

4.	On December 1, 2018, AT&T swapped Mr. Williams' SIM card without his authorization. (*See e.g.* Appendix, Ex. 1 at ATT-WIL-00668 (AT&T Account Note entitled "Replace SIM"); Ex. 2.)		
5.	On December 4, 2018, AT&T swapped Mr. Williams' SIM card without his authorization. (*See e.g.* Appendix, Ex. 1 at ATT-WIL-00658 (AT&T Account Note entitled "Replace SIM"); Ex. 2.)		
6.	On February 4, 2019, AT&T swapped Mr. Williams' SIM card without his authorization. (*See e.g.* Appendix, Ex. 1 at ATT-WIL-00649 (AT&T Account Note entitled "Replace SIM"); Ex. 2.)		
7.	On February 6, 2019, AT&T swapped Mr. Williams' SIM card without his authorization. (*See e.g.* Appendix, Ex. 1 at ATT-WIL-00647 (AT&T Account Note entitled "Replace SIM"); Ex. 2.)		
8.	On February 8, 2019, AT&T swapped Mr. Williams' SIM card without his authorization. (*See e.g.* Appendix, Ex. 1 at ATT-WIL-00641 (AT&T Account Note entitled "Replace SIM").)		
9.	After the final SIM swap, in February 2019, Mr. Williams realized he could no longer trust AT&T to protect his account and switched his cell phone provider from AT&T to Verizon, keeping the same phone number. (Appendix, Ex. 3 at 271:10-274:21; 304:12-305:22; Ex. 5 at 1-3.)		
10.	Since switching from AT&T to Verizon, Mr. Williams has not		

	been subject to any additional SIM swaps. (Appendix, Ex. 3 at 271:10-274:21; 304:12-305:22; Ex. 5 at 1-3.)		
11.	In or about November 2018, on a phone call between Mr. Williams and AT&T, AT&T represented that it would add extra security to Mr. Williams' account by making changes and notations in his account, whereby the SIM card associated with his account could only be changed via an in-person request in a specific, identified Raleigh AT&T store. (Appendix, Ex. 5 at 2; *see* Ex. 3 at 304:12-305:22.)		
12.	In or about November 2018, on a phone call between Mr. Williams and AT&T, AT&T represented that Mr. Williams' identity would have to be confirmed with two passports before AT&T would approve a SIM card change on his account. (Appendix, Ex. 5 at 2; *see* Ex. 3 at 304:12-305:22.)		
13.	On or about December 2, 2018, at AT&T store in Raleigh, an AT&T employee said that certain warnings regarding Mr. Williams' account must be getting deleted from his AT&T account. (Appendix, Ex. 5 at 2; *see* Ex. 3 at 304:12-305:22.)		
14.	On or about December 2, 2018, at AT&T store in Raleigh, an AT&T employee told Mr. Williams that he was on a special list of individuals who were at high risk of being SIM swapped. (Appendix, Ex. 5 at 2; *see* Ex. 3 at 304:12-305:22.)		
15.	On or about December 2, 2018, on a phone call between Mr. Williams and AT&T, an AT&T representative told Mr. Williams		

	that certain warnings that had been placed on his account were erased from his account, but could not provide any explanation as to why. (Appendix, Ex. 5 at 2; *see* Ex. 3 at 304:12-305:22.)		
16.	On or about December 5, 2018, at AT&T store in Raleigh, AT&T employees told Mr. Williams that there was a note in his account regarding SIM swap procedures. (Appendix, Ex. 5 at 3; *see* Ex. 3 at 304:12-305:22.)		
17.	AT&T's account notes associated with Mr. Williams' phone number contain a November 6, 2018, entry entitled "Special Instructions" that states: "Customer was previous victim of Account Takeover on 11/05/18. Please use caution when making account changes/placing order." (Appendix, Ex. 1 at ATT-WIL-00676.)		
18.	AT&T's account notes associated with Mr. Williams' phone number contain a December 3, 2018, entry entitled "Special Instructions" that states: "Customer has verified himself with ID and passcode with manager. Customer has given instructions that transactions can only be made in person with ID and passcode verification… Do not verify by last 4 of ssn….12/03/18 **FRAUD DEPT DO NOT REMOVE** Customer was previous victim of Account Takeover on xx/xx/xx. Please use caution when making account changes/placing order." (Appendix, Ex. 1 at ATT-WIL-00663.)		
19.	AT&T's account notes associated with Mr. Williams' phone number contain a December 5, 2018 entry entitled "Special		

	Instructions" that states: "*FRAUD DEPT DO NOT REMOVE** Account holder lives in NC state and scammers went to OK state att cor store with ID to update sim card multiple times! AH is requesting to verify both the NC state issued driver license and passport before changing sim cards or make changes to the account!" (Appendix, Ex. 1 at ATT-WIL-00656.)		
20.	AT&T's account notes associated with Mr. Williams' phone number contain February 4, 2019, entry entitled "Special Instructions" that states: "TO ACCESS THE ACCOUNT MUST IDENTIFY ACCOUNT HOLDER VIA 2 PASSPORTS AND I.D. Do not make any changes over the phone at the request Jason Williams verified in store with 2 passports and 1 drivers license." (Appendix, Ex. _ at ATTWIL-00649.)		
21.	Robert Arno, an AT&T employee who investigates SIM swaps and other types of fraud, testified that the most recently added "Special Instructions" notation for a particular customer account appears prominently in the system that AT&T employees use view that customer's account notes. (Appendix, Ex. 6 at 154:10-157:20.)		
22.	By November 2018, AT&T knew, or should have known, that unauthorized SIM swaps were serious threats to its customers. (*See* Appendix, Ex. 7; Ex. 8; Ex. 9; Ex. 10.)		
23.	In his expert report on behalf of AT&T, Richard Sanders wrote: "…Mr. Williams sought to obtain assurances of special treatment		

	from employees at an AT&T retail store in Raleigh, NC. Mr. Williams alleges he relied on statements by those store employees that extra security would be added to his account, and that future requests for SIM changes would have to be made in person and with two forms of identification. Mr. Williams knew or should have known that these measures could not guarantee he would not be SIM swapped again." (*See* Appendix, Ex. 7 at 36-37.)		
24.	In his expert report on behalf on AT&T, Richard Sanders wrote: "By November 2018, it was widely reported in news media online that such measures cannot guarantee a SIM swap will not happen, particularly if it is done by an insider." (*See* Appendix, Ex. 7 at 37.)		
25.	The November 5, 2018, SIM swap on Mr. Williams' account was performed by an AT&T agent named Stephen Defiore. (*See e.g.* Appendix, Ex. 1 at ATT-WIL-00678; Ex. 4 at 131:12-134:19.)		
26.	Defiore was an employee at Prime Communications, an authorized AT&T retailer. (*See* Appendix, Ex. 11 at 2; Ex. 12.)		
27.	AT&T's 30(b)(6) deponent regarding the topic of Mr. Williams' SIM swaps, Ray Hill, AT&T Director Project Program Management, testified that Defiore was a "manager." (*See e.g.* Appendix, Ex. 4 at 131:12-134:19.)		
28.	On September 18, 2019, Dan Haley, a Prime Communications Senior Loss Prevention Manager, sent an email to Ray Hill, then apparently with the title AT&T		

	Associate Director – Compliance (Retail), regarding Stephen Defiore. (Appendix, Ex. 12.)		
29.	In his September 18, 2019, email to Ray Hill, Dan Haley wrote: "Thru video footage and account research, I found that only Stephen Defiore was involved in unauthorized sim card changes. Defiore took full responsibility for all sim card changes that we were made aware of by At&t [sic]." (Appendix, Ex. 12.)		
30.	Ray Hill testified that Defiore, and other AT&T agents operating in a "retail environment," had the ability to change any AT&T customer's SIM card by simply entering the last four digits of the customer's social security number and noting, without verification, that they had reviewed the customer's photo identification. (*See e.g.* Appendix, Ex. 4 at 148:24-152:1.)		
31.	Mr. Williams was and is the sole member of Apollo Kids Mining, LLC ("Apollo"), through which he operated a successful Bitcoin mining operation. (*See* Appendix, Ex. 3 at 25:19-24; 231:25-235:4; 237:5-19.)		
32.	Williams was entitled to all of the proceeds from Apollo and its Bitcoin mining operation. (*See* Appendix, Ex. 3 at 25:19-24; 231:25-235:4; 237:5-19.)		
33.	All of the proceeds from Mr. Williams' Bitcoin mining operation were deposited directly into online cryptocurrency accounts, each of which was accessed via Mr. Williams' personal email, and subject to his sole control.		

	(*See* May 2, 2022, Declaration of Jason Williams ("Williams Decl.") ¶¶2-3; Appendix, Ex. 13; Ex. 14 at 4-7.)		
34.	Mr. Williams's cryptocurrency accounts received the proceeds from his Apollo Bitcoin mining operation, as well as cryptocurrency he received from other sources. (Williams Decl. ¶4)		
35.	As a result of the AT&T's first SIM swap of Mr. Williams' account, hackers were able to divert his Apollo Bitcoin mining operation proceeds from Mr. Williams' cryptocurrency accounts to an account (or accounts) controlled by the hackers. (*See* Appendix, Ex. 2; Ex. 14 at 4-5; Ex. 3 at 90:24-92:5.)		
36.	After AT&T's repeated SIM swaps of Mr. Williams' account compromised the safety of this mining operation, Mr. Williams was forced to discontinue it, or risk attacks against his other (as yet un-hacked) operations. (*See* Appendix, Ex. 14 at 11-14; Ex. 3 at 256:9-259:19.)		
37.	As a result of the SIM swaps, Mr. Williams received threatening calls and text message from unknown individuals. (Appendix, Ex. 15.)		
38.	As a result of the SIM swaps, Mr. Williams received threatening calls and text messages from unknown individuals. (Appendix, Ex. 15.)		
39.	As a result of the SIM swaps, Mr. Williams received a text message threatening that his daughter would be kidnapped. (Appendix, Ex. 3 at 67:17-68:18; 72:14-73:6; Ex. 16 ("Answer the		

	phone or your daughter will go missing tonight."))		
40.	When Mr. Williams contacted the local police about the kidnapping threat, they told him they could not protect him or his family. (Appendix, Ex. 3 at 61:7-62:24.)		
41.	The local police told Mr. Williams to be "ready to use" a gun to protect himself and his family. (Appendix, Ex. 3 at 61:7-62:24.)		
42.	As a result of the SIM swaps, Mr. Williams purchased a gun, silencer, and other firearm accessories in response to the threats that followed the SIM swaps. (Appendix, Ex. 17.)		
43.	After the first SIM swap, agents at the FBI told Mr. Williams that his and his family's personal information had been released onto the "Dark Web," where it was available to criminals and hackers. Appendix, Ex. 3 at 112:11-22; 173:18-22; 259:10-263:11.)		
44.	As a result of the SIM swaps, criminals used Mr. Williams' phone number to impersonate him and convince an acquaintance and business associate to transfer Bitcoin to them, harming his reputation in the process. (Appendix, Ex. 18.)		
45.	As a result of the SIM swaps, Mr. Williams' online accounts, including his personal Gmail account, and the information within those accounts, were compromised by hackers. (Appendix, Ex. 19 at 5-7; Ex. 3 at 117:8-130:7; Ex. 20; *see also* Ex. 31 (showing that hackers took control of Mr. Williams Coinbase		

	account, and changed the email address associated with that account to a proton.com email address that did not belong to Mr. Williams)		
46.	Mr. Williams has never been able to recover his personal Gmail account since the SIM swap attacks. (Appendix, Ex. 19 at 5-7; Ex. 3 at 117:8-130:7; Ex. 20.)		
47.	Mr. Williams testified: "Specifically the night or the afternoon that I was threatened by text message, that if I didn't respond or do something, that my daughter would go missing. I called the police.· I was terrified." (Appendix, Ex. 3 at 61:16-21.)		
48.	Mr. Williams testified: "So it was highly disruptive to, you know, me being a fund manager and having to deal with this….And as you can imagine, me being a target of SIM swaps and this level of instability, you know, threatened my ability to be a good steward of my responsibilities with these people. It was highly -- it was highly disruptive.· It was something that – it was just a very, very big deal. I wish I had the capacity and the words to explain to you how unnerving this is. This is my life. It's what I worked toward. I don't practice medicine anymore. This is what I do, and for me to have my personal information coopted for these folks to reach out to business clients and to solicit money and try to extract like business deals and doings that have nothing to do with me, it's just terrifying." (Appendix, Ex. 3 at 66:8-67:9 .)		
49.	Mr. Williams testified: "Throw on top of it you are worried about your safety and your family's safety. It's terrifying. I hate to		

	keep using the same word, but it is very scary." (Appendix, Ex. 3 at 70:15-18.)		
50.	Mr. Williams testified: "I had never experienced something like this. I have got ten plus businesses that I'm running, and this is my first experience with this kind of Dark Web hacker kind of thing affecting me so close to home." (Appendix, Ex. 3 at 165:13-18.)		
51.	Mr. Williams testified: "I think what I'm saying to you is a [sic] threatening a 15 year old to be kidnapped and having police with guns in your house and your father trying to project himself as some type of vigilante who can defend himself with weapons, who is tired, exhausted from this, and it's affected me. It's affected my relationships. It's affected my daughter. It's affected me and my wife. I am making that claim. How do I quantify that? I don't know. Do I think you are liable, yes. Yes, 100 percent. Do I think that these SIM swaps have taken a toll on me, and have affected my businesses negatively, yes. How do I quantify that? I don't know. I'm leaving that up to these attorneys. That's why I persisted. That's why I'm sitting here today and that's why I'm willing to go to trial with this. (Appendix, Ex. 3 at 248:22-249:19.)		
52.	Mr. Williams gave a podcast interview in which he described the effects of the SIM swaps to an interviewer, and told the interviewer: "It's frightening." (Appendix, Ex. 24 at ATT-WIL-02319.)		
53.	Mr. Williams believes, based on his experience of the SIM swaps and their aftermaths, that the threats, privacy breaches, and		

	fears that he and his family experienced in late 2018 and early 2019 were entirely related to the SIM swaps. (Williams Decl. ¶5)		
54.	Before November 5, 2018, the day AT&T first SIM swapped Mr. Williams' phone, he never received text messages and phone calls threatening him and his family. (Williams Decl. ¶5)		
55.	Before November 5, 2018, to Mr. Williams' knowledge, no one ever impersonated him online or over the phone. (Williams Decl. ¶5)		
56.	Before November 5, 2018, to Mr. Williams' knowledge, his online accounts, including his bank accounts and his personal email containing over a decades' worth of his personal and financial information, had never been hacked and compromised. (Williams Decl. ¶5)		
57.	Before November 5, 2018, Mr. Williams had no reason to believe that any of his personal or financial information was available to criminals on the "Dark Web." (Williams Decl. ¶5)		
58.	During the period that Mr. Williams was subject to AT&T's SIM swaps, between November 2018 and February 2019, there were many nights when he was unable to sleep because he was so afraid for his and his family's safety. (Williams Decl. ¶6)		
59.	During those nights, Mr. Williams would stay awake with a gun in hand because he was afraid intruders would come to		

	his home and attempt to harm him or his family. (Williams Decl. ¶6)		
60.	Mr. Williams' fears seemed, and still seem, reasonable to him in light of threats he received, and the scale of the security and privacy breaches that occurred as a result of the SIM swaps. (Williams Decl. ¶6)		
61.	Since Mr. Williams switched to Verizon, he has no longer had to deal with SIM swaps on his phone, or active hacking attempts on his online accounts. This may be due to Verizon's security efforts, or to his own continuing security efforts. (Williams Decl. ¶7)		
62.	The fear of what criminals and hackers might do with the personal and financial information that AT&T gave them access to, and how they could use that information to compromise the safety, security, and privacy of Mr. Williams and his family, has not gone away, and he does not suspect it ever will. As just one example, he continues to fear that those criminals who accessed and used his personal email account, and a decade's worth of my personal emails, will use that information to harm or extort him and his family. (Williams Decl. ¶7)		
63.	In a letter dated May 14, 2019, addressed to Mr. Williams, from Tami Shurtz, AT&T Senior Manager – Office of the President, Ms. Shurtz wrote: "We recently determined that an employee of one of our service providers accessed your Customer Proprietary Network Information (CPNI) without authorization."		

	(Appendix, Ex. 25.)		
64.	In a letter dated July 3, 2019, addressed to Mr. Williams, from Nena Romano, Director, Compliance – AT&T Communications, Ms. Romano wrote: "We recently determined that an employee of one of our service providers accessed your Customer Proprietary Network Information (CPNI) without authorization." (Appendix, Ex. 26.)		
65.	In public facing customer information and internal AT&T documents, AT&T has acknowledged that its customers use two-factor authentication, including two-factor authentication involving phone calls and text messages as "an extra security layer" for their online accounts. (Appendix, Exs. 27 and 28.)		

Respectfully submitted this 2nd day of May, 2022.

Christopher N. LaVigne
Joseph Gallo
Withers Bergman LLP
430 Park Avenue, 10th Floor
New York, New York 10022-3505
Telephone: (212) 848-9800
Facsimile: (212) 848-9888
christopher.lavigne@withersworldwide.com
joseph.gallo@withersworldwide.com
State Bar No. NY 4811121

Counsel for Plaintiff Jason Williams

Terence S. Reynolds
Lucas Garber
SHUMAKER LOOP & KENDRICK LLP
101 South Tyron Street, Suite 2200
Charlotte, North Carolina 28280
Telephone: (704) 375-0057
Facsimile: (704) 332-1197
treynolds@shumaker.com
State Bar No. 49848

Local Civil Rule 83.1(d) Counsel for Plaintiff Jason Williams

CERTIFICATE OF SERVICE

I hereby certify that on date set out below, I electronically filed the foregoing document with the Clerk of Court using the CM/ECF system which will send notification of such filing to the following:

Nancy L. Stagg (CA State Bar No. 157034)
KILPATRICK TOWNSEND & STOCKTON LLP
12255 El Camino Real, Suite 250
San Diego, CA 92130
Telephone: (858) 350-6156
Facsimile: (858) 350-6111
Email: nstagg@kilpatricktownsend.com

Joseph S. Dowdy (N.C. State Bar No. 31941)
KILPATRICK TOWNSEND & STOCKTON LLP
4208 Six Forks Road, Suite 1400
Raleigh, NC 27609
Telephone: (919) 420-1700
Facsimile: (919) 510-6120
Email: jdowdy@kilpatricktownsend.com

Michael Breslin (GA State Bar No. 142551)
KILPATRICK TOWNSEND & STOCKTON LLP
1100 Peachtree St. NE, Suite 2800
Atlanta, GA 30309
Telephone: (404) 815-6500
Facsimile (404) 815-6555
Email: mbreslin@kilpatricktownsend.com

Counsel for Defendant AT&T Mobility LLC

This the 2nd day of May, 2022

/s/ Christopher LaVigne
Christopher LaVigne